

A note on the Singleton bounds for codes over finite rings*

Yongsheng Tang¹, Heqian Xu¹, Zhonghua Sun²

¹*School of Mathematics and Statistics, Hefei Normal University, Hefei 230601, Anhui, P.R.China*

²*School of Mathematics, Hefei University of Technology, Hefei 230009, Anhui, P.R.China*

Abstract In this paper, we give a notation on the Singleton bounds for linear codes over a finite commutative quasi-Frobenius ring in the work of Shiromoto [5]. We show that there exists a class of finite commutative quasi-Frobenius rings. The Singleton bounds for linear codes over such rings satisfy

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

keywords: Linear codes, General weight, Quasi-Frobenius ring, Singleton bounds

1 Introduction

Let R be a finite commutative quasi-Frobenius (QF) ring with characteristic k and cardinality M , where $k = \prod_{i=1}^s p_i^{t_i}$, $M = \prod_{i=1}^s p_i^{r_i t_i}$, p_i are distinct primes, r_i and t_i are positive integers (see [4] and [7]). Let R^n be the free R -module of rank n consisting of all n -tuples of elements of R . A linear code C of length n over R is a R -submodule of R^n . An element of C is called a codeword of C . In this paper, we will use a general notion of weight, abstracted from the Hamming, the Lee and the Euclidean weights. For each $c = (c_1, c_2, \dots, c_n) \in R^n$ and $r \in R$, the complete weight of c is defined by

$$n_r(c) = \{i | c_i = r\}.$$

To define a general weight function $w(c)$, let a_r , $(0 \neq) r \in R$ be positive real numbers, and set $a_0 = 0$. Set

$$w(c) = \sum_{r \in R} a_r n_r(c). \quad (1)$$

If we set $a_r = 1$, for every $(0 \neq) r \in R$, then $w(c)$ is just the Hamming weight of c , denoted by $w_H(c)$. Throughout this paper, we denote

$$A = \max\{a_r | r \in R\}. \quad (2)$$

For a linear code C , the general weight distance, denoted by $d(C)$, is equal to the minimum general weight $w(C)$ of the code C .

Example 1.1. Let us consider the ring $R = \mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. If we set $a_0 = 0, a_1 = a_5 = 1, a_2 = a_4 = 2$ and $a_3 = 3$, which yield the Lee weights of the elements of \mathbb{Z}_6 (see [6]). Then $A = 3$. While if we set $a_0 = 0, a_1 = a_5 = 1, a_2 = a_4 = 4$ and $a_3 = 9$, which yield the Euclidean weights of the elements of \mathbb{Z}_6 , then $A = 9$.

Example 1.2. Let us consider the ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}$, which is a 2-dimensional algebra over the field \mathbb{F}_2 with a nilpotent element u where $u^2 = 0$ (see [1]). If we set

* E-mail addresses: ysh_tang@163.com(Y. Tang), 693204301@qq.com(H. Xu), 1191398576@qq.com(Z. Sun).

$a_0 = 0, a_1 = a_{1+u} = 1$ and $a_u = 2$, which yield the Lee weights of the elements of $\mathbb{F}_2 + u\mathbb{F}_2$. Then $A = 2$. While if we set $a_0 = 0, a_1 = a_{1+u} = 1$ and $a_u = 4$, which yield the Euclidean weights of the elements of $\mathbb{F}_2 + u\mathbb{F}_2$, then $A = 4$.

The following Singleton bounds on a general weight function for linear code C over a finite commutative QF ring were obtained in [5].

Theorem 1.3. *Let C be a linear code of length n over a finite commutative QF ring R . Let $w(c)$ be a general weight function on C , as in (1); and with maximum a_r -value A , as in (2). Suppose the minimum general weight of $w(c)$ on C is $d(C)$. Then*

$$\left\lfloor \frac{d(C) - 1}{A} \right\rfloor \leq n - \log_{|R|} |C|,$$

where $[b]$ is the integer part of b .

The purpose of this paper is to show that there exists a class of finite commutative QF rings. The Singleton bounds for linear codes over such rings satisfy

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

2 General Gray map on R

Let R be a finite commutative quasi-Frobenius (QF) ring with characteristic k and cardinality M , where $k = \prod_{i=1}^s p_i^{t_i}$, $M = \prod_{i=1}^s p_i^{r_i t_i}$, p_i are distinct primes, r_i and t_i are positive integers. For any element $a \in R$, a general Gray map φ on R is defined as

$$\varphi : R \rightarrow \mathbb{F}_{p_i^{e_i}}^A,$$

$$a \mapsto (a_1, \dots, a_i, a_{i+1}, \dots, a_A),$$

where $p_i^{e_i}$ is any divisor of $\prod_{i=1}^s p_i^{r_i t_i}$ and $\mathbb{F}_{p_i^{e_i}}$ is a finite field with $p_i^{e_i}$ elements. In detail,

- if $a_0 = 0$, $w(0) = 0$, then $\varphi(0) = (0, \dots, 0, 0, \dots, 0)$;
- if $0 < a_r < A$ and $w(a_r) = i$, then $\varphi(a_r) = (a_1, \dots, a_i, a_{i+1}, \dots, a_A)$, where there are i nonzeros and $A - i$ zeros among $a_1, \dots, a_i, a_{i+1}, \dots, a_A$;
- if $a_r = A$ and $w(a_r) = A$, then $\varphi(a_r) = (a_1, \dots, a_i, a_{i+1}, \dots, a_A)$, where $a_t \neq 0$ for $t = 1, 2, \dots, A$.

The general Gray map φ can be extended to R^n in an obvious way.

Example 2.1. Let us consider a general Gray map φ on \mathbb{Z}_6 with the Lee weight. From Example 1.1, we have $A = 3$. A general Gray map φ from \mathbb{Z}_6 to \mathbb{F}_m^3 ($m = 2$ or 3), can be defined as $\varphi(0) = (0, 0, 0)$, $\varphi(1) = (0, 0, a_{11})$, $\varphi(2) = (0, a_{21}, a_{22})$, $\varphi(3) = (a_{31}, a_{32}, a_{33})$, $\varphi(4) = (a_{41}, a_{42}, 0)$, $\varphi(5) = (a_{51}, 0, 0)$, where $a_{ij} \neq 0$.

From the definition of the general Gray map we can obtain the following theorem.

Theorem 2.2. *Let the notation be as before. For any finite commutative QF ring R , there*

exists a Gray map φ from R^n to $\mathbb{F}_{p_i^{e_i}}^{An}$ and the Gray map φ is a distance preserving map from $(R^n, \text{general weight distance})$ to $(\mathbb{F}_{p_i^{e_i}}^{An}, \text{Hamming distance})$.

Proof. From the above definitions, it is clear that $\varphi(x - y) = \varphi(x) - \varphi(y)$ for $x, y \in R^n$. Thus, $d(x, y) = w(x - y) = w_H(\varphi(x - y)) = w_H(\varphi(x) - \varphi(y)) = d_H(\varphi(x), \varphi(y))$. \square

3 Main result

In this section, we will show that there exists a class of finite commutative QF rings. The Singleton bounds for linear codes over such rings satisfy

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

For our purpose, we firstly introduce the following lemma on the Singleton bounds for codes over finite fields (see [3]).

Lemma 3.1. *Let C be a code (possibly nonlinear) of length n over the finite field \mathbb{F}_q with $|C|$ elements and the minimum Hamming distance $d_H(C)$. Then*

$$d_H(C) \leq n - \log_q |C| + 1.$$

Theorem 3.2. *Let C be a linear code of length n over a finite commutative QF ring R . Let $w(x)$ be a general weight function on C , as in (1); and with maximum a_r -value A , as in (2). Suppose the minimum weight of $w(x)$ on C is $d(C)$. Let $p = \min\{p_1, \dots, p_s\}$ and φ be a distance preserving map from $(R^n, \text{general weight distance})$ to $(\mathbb{F}_{p_i^{e_i}}^{An}, \text{Hamming distance})$. Then*

$$d(C) \leq An - \log_p |C| + 1.$$

Furthermore, if φ is a bijective map and a distance preserving map from $(R^n, \text{general weight distance})$ to $(\mathbb{F}_p^{An}, \text{Hamming distance})$, then

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

Proof. By Theorem 2.2, we have each general Gray image of the code C under its corresponding general Gray map φ is a $p_i^{e_i}$ -ary code with the same length An and the same minimum Hamming distance $d_H(\varphi(C))$. By Lemma 3.1, each general Gray image of the code C satisfies

$$d_H(\varphi(C)) \leq An - \log_{p_i^{e_i}} |\varphi(C)| + 1.$$

Furthermore

$$d(C) = d_H(\varphi(C)) \leq \min\{An - \log_{p_i^{e_i}} |\varphi(C)| + 1\} = An - \max\{\log_{p_i^{e_i}} |\varphi(C)|\} + 1.$$

Since $p = \min\{p_1, \dots, p_s\}$ and $|\varphi(C)| \leq |C|$, then $\max\{\log_{p_i^{e_i}} |\varphi(C)|\} = \log_p |C|$. Therefore

$$d(C) \leq An - \log_p |C| + 1.$$

On the other hand, if φ is a bijection from R^n to \mathbb{F}_p^{An} , then $\log_{p^{e_i}} |\varphi(C)|$ is maximum, that is, if $\log_{p^{e_i}} |\varphi(C)|$ attains to be maximum, then $|R| = p^A$ and $|\varphi(C)| = |C|$. Hence, we have

$$d(C) \leq An - \log_p |C| + 1.$$

It follows that

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

This completes the proof. \square

Remark 3.2 Theorem 3.2 shows that if there exists a bijective map φ and the map φ is a distance preserving map from $(R^n, \text{general weight distance})$ to $(\mathbb{F}_p^{An}, \text{Hamming distance})$, then the Singleton bounds for linear codes over R satisfy

$$\frac{d(C) - 1}{A} \leq n - \log_{|R|} |C|.$$

Example 3.3. Consider any linear code C of length $n(\geq 1)$ over the QF ring $\mathbb{F}_2 + u\mathbb{F}_2 = \{0, 1, u, 1 + u\}$. The Lee weights of the elements of $\mathbb{F}_2 + u\mathbb{F}_2$ is given as follows: $w_L(0) = 0$, $w_L(1) = 1$, $w_L(u) = 2$, $w_L(1 + u) = 1$. For any element $a + ub \in \mathbb{F}_2 + u\mathbb{F}_2$. A Gray map φ from $\mathbb{F}_2 + u\mathbb{F}_2$ to \mathbb{F}_2^2 is defined as $\varphi(a + ub) = (b, a + b)$ (see [1]). The map φ can be extended to $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ in an obvious way and the extended φ is a bijection from $(\mathbb{F}_2 + u\mathbb{F}_2)^n$ to \mathbb{F}_2^{2n} . Therefore, we have

$$\frac{d(C) - 1}{2} \leq n - \log_4 |C|.$$

Example 3.4. Consider any linear code C of length $n(\geq 1)$ over the QF ring $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, which is a characteristic 2 ring subject to the restrictions $u^2 = v^2 = 0$ and $uv = vu$. Let $\varphi : (\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2)^n \rightarrow \mathbb{F}_2^{4n}$ be the map given by $\varphi(a + ub + vc + uvd) = (a + b + c + d, c + d, b + d, d)$. Then φ is a bijective map. For any element $a + ub + vc + uvd \in \mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, we define the Lee weight $w_L(a + ub + vc + uvd) = w_H(a + b + c + d, c + d, b + d, d)$, where w_H denotes the ordinary Hamming weight for binary codes (see [8]). Therefore, we have

$$\frac{d(C) - 1}{4} \leq n - \log_{16} |C|.$$

4 An application to codes over \mathbb{Z}_ℓ

In this section, we mainly introduce the ring \mathbb{Z}_ℓ as a good example of a finite commutative QF ring. Let $\mathbb{Z}_\ell = \{0, 1, \dots, \ell - 1\}$ denote the ring of integers modulo ℓ . Now we introduce three kinds of weights, namely the Hamming weight, the Lee weight, and the Euclidean weight. The Hamming weight $w_H(c)$ of a vector $c = (c_1, c_2, \dots, c_n) \in \mathbb{Z}_\ell^n$, is the number of its nonzero entries in the vector. The Lee weight for the elements of \mathbb{Z}_ℓ is defined as $w_L(a) = \min\{a, \ell - a\}$ for all $a \in \{0, 1, \dots, \ell - 1\}$ (see [6]). The Euclidean weight for the elements of \mathbb{Z}_ℓ is defined as $w_E(a) = w_L(a)^2$ for all $a \in \{0, 1, \dots, \ell - 1\}$. Denote the minimum weight of a linear code C with respect to Hamming, Lee, Euclidean weights by $d_H(C)$; $d_L(C)$ and $d_E(C)$; respectively. It is clear that the maximum a_r -value is 1; $\lfloor \ell/2 \rfloor$ and $\lfloor \ell/2 \rfloor^2$; respectively. In the following, we denote by ℓ_1 and ℓ_2 the following integers, respectively, $\ell_1 = \lfloor \ell/2 \rfloor$ and $\ell_2 = \lfloor \ell/2 \rfloor^2$.

The next result follows immediately from Theorem 3.2.

Corollary 4.1. *Let C be a linear code of length n over \mathbb{Z}_ℓ , where $\ell = \prod_{i=1}^s p_i^{a_i}$, p_i are distinct primes and a_i are positive integers. Let $p = \min\{p_1, \dots, p_s\}$. Then there are the following bounds on minimum weights:*

$$\begin{aligned} d_H(C) &\leq n - \log_p |C| + 1; \\ d_L(C) &\leq \ell_1 n - \log_p |C| + 1; \\ d_E(C) &\leq \ell_2 n - \log_p |C| + 1. \end{aligned}$$

Furthermore, if φ is a bijective map and a distance preserving map from $(\mathbb{Z}_\ell^n, \text{general weight distance})$ to $(\mathbb{F}_p^{A_n}, \text{Hamming distance})$, then

$$\begin{aligned} d_H(C) - 1 &\leq n - \log_\ell |C|; \\ \frac{d_L(C) - 1}{\ell_1} &\leq n - \log_\ell |C|; \\ \frac{d_E(C) - 1}{\ell_2} &\leq n - \log_\ell |C|. \end{aligned}$$

Example 4.2. Consider any linear code C of length $n(\geq 1)$ over the QF ring $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. The Lee weights of the elements of \mathbb{Z}_4 are given as follows: $w_L(0) = 0$, $w_L(1) = w_L(3) = 1$, $w_L(2) = 2$. Then $A = 2$. There exists a bijective map φ from \mathbb{Z}_4 to \mathbb{F}_2^2 . In fact, $\varphi(0) = (0, 0)$, $\varphi(1) = (0, 1)$, $\varphi(2) = (1, 1)$, and $\varphi(3) = (1, 0)$ (see [2]). The map φ can be extended to \mathbb{Z}_4^n in an obvious way and the extended φ is a bijection from \mathbb{Z}_4^n to \mathbb{F}_2^{2n} . Therefore, we have

$$\frac{d_L(C) - 1}{2} \leq n - \log_4 |C|.$$

Acknowledgements

This research is supported by Natural Science Foundation of Anhui Province (No. 1408085QF116), Colleges Outstanding Young Talents Program in 2014, Anhui Province (No. [2014]181) and Hefei Normal University Research Project (No. 2015JG09).

References

- [1] A. Bonnetcaze, P. Udaya, Cyclic codes and self-dual codes over $\mathbb{F}_2 + u\mathbb{F}_2$, *IEEE Trans. Inform. Theory* **4** (1999) 1250-1255.
- [2] A.R. Hammons, P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The \mathbb{Z}_4 -linearity of Kerdock, Preparata, Goethals, and Related Codes, *IEEE Trans. Inform. Theory* **40** (1994) 301-319.
- [3] F.J. Macwilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland, Amsterdam New York, 1977.
- [4] B. R. McDonald, *Finite Rings with Identity*, Dekker, New York, 1974.

- [5] K. Shiromoto, Singleton bounds for codes over finite rings, *Journal of Algebraic Combinatorics* **12** (2000) 95-99.
- [6] J.H. Van Lint, *Introduction to Coding Theory*, Third ed., Springer, Berlin, 1999.
- [7] J. Wood, Duality for modules over finite rings and applications to coding theory, *American Journal of Mathematics* **121** (1999) 555-575.
- [8] B. Yildiz, S.Karadeniz, Linear codes over $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$, *Des. Codes Cryptogr.* **54** (2010)61-81.